Amendments to the Claims

1. (Currently Amended) A method of providing distributed web server authentication ~~of a valid user requesting access to a web server~~, said method comprising:
receiving a request to connect a valid user to a web server;
creating a user password cookie using a shared secret key, wherein the web server is part of a common authentication ring having a plurality of web servers, each of the plurality of web servers having the shared secret key; and
transmitting the user password cookie in response to the request to connect.

2. (Original) The method of claim 1, wherein creating a user password cookie using a shared secret key, comprises:
reading a user credential cookie;
requesting a user identification (ID) and password;
receiving the user ID and password; and
validating the valid user's identity.

3. (Original) The method of claim 2, wherein validating the valid user's identity, comprises:
authenticating the user ID and password with the user credential cookie using a local authenticating mechanism.

4. (Previously Amended) The method of claim 3, wherein the local authenticating mechanism comprises an operating system.

5. (Original) The method of claim 2, wherein creating a user password cookie using the shared secret key, further comprises:
combining at least the user ID and password with a time stamp; and
encrypting the combined at least user ID, password and time stamp using the shared secret key.

6. (Original) The method of claim 1, wherein creating a user password cookie using a shared secret key, comprises:
obtaining the user password cookie;
verifying that the user password cookie is valid; and
updating the user password cookie using the shared secret key.

7. (Original) The method of claim 6, wherein updating the user password cookie using the shared secret key, comprises:
combining at least a user identification (ID) and password with a time stamp; and
encrypting the combined at least user ID, password and time stamp using the shared secret key.

8. (Cancelled)

9. (Original) The method of claim 1, further comprising:
authenticating a second valid user requesting access to the web server.

10. (Original) The method of claim 9, wherein authenticating a second valid user requesting access to the web server, comprises:
receiving a request to connect the second valid user to the web server; and
creating a second user password cookie using the shared secret key; and
transmitting the second user password cookie in response to the request to connect the second valid user.

11. (Currently Amended) The method of claim 1, further comprising:
authenticating the valid user at a second web server, wherein the web server and the second web server are part of ~~a~~ the common authentication ring.

12. (Original) The method of claim 11, wherein authenticating the valid user at a second web server, comprises:
receiving a request to connect the valid user to the second web server;
updating the user password cookie using the shared secret key; and
transmitting the user password cookie in response to the request to connect the valid user to the second web server.

13. (Currently Amended) A computer-readable medium having stored therein a computer program for providing distributed web server authentication of a valid user requesting access to a web server, said program comprising instructions for:
receiving a request to connect the valid user to the web server;
creating a user password cookie using a shared secret key, wherein the web server is part of a common authentication ring having a plurality of web servers, each of the plurality of web servers having the shared secret key; and
transmitting the user password cookie in response to the request to connect.

14. (Original) The computer-readable medium of claim 13, wherein creating a user password cookie using a shared secret key, comprises:
reading a user credential cookie;
requesting a user identification (ID) and password;
receiving the user ID and password; and
validating the valid user's identity.

15. (Original) The computer-readable medium of claim 14, wherein validating the valid user's identity, comprises:
authenticating the user ID and password with the user credential cookie using a local authenticating mechanism.

16. (Previously Amended) The computer-readable medium of claim 15, wherein the local authenticating mechanism comprises an operating system.

17. (Original) The computer-readable medium of claim 14, wherein creating a user password cookie using the shared secret key, further comprises:
combining at least the user ID and password with a time stamp; and
encrypting the combined at least user ID, password and time stamp using the shared secret key.

18. (Original) The computer-readable medium of claim 13, wherein creating a user password cookie using a shared secret key, comprises:
obtaining the user password cookie;
verifying that the user password cookie is valid; and
updating the password cookie using the shared secret key.

19. (Original) The computer-readable medium of claim 13, further comprising:
authenticating a second valid user requesting access to the web server.

20. (Previously Amended) The computer-readable medium of claim 19, wherein authenticating a second valid user requesting access to the web server, comprises:
receiving a request to connect the second valid user to the web server;
creating a second user password cookie using the shared secret key; and
transmitting the second user password cookie in response to the request to connect the second valid user.

21. (Currently Amended) The computer-readable medium of claim 13, further comprising:
authenticating the valid user at a second web server, wherein the web server and the second web server are part of a the common authentication ring.

22. (Original) The computer-readable medium of claim 21, wherein authenticating the valid user at a second web server, comprises:
receiving a request to connect the valid user to the second web server;
updating the user password cookie using the shared secret key; and
transmitting the user password cookie in response to the request to connect the valid user to the second web server.

23. (Original) A computer-readable medium encoded with a data structure representing a password cookie, said data structure comprising:
a user identification (ID);
a password; and
a time stamp associated with said user ID and password, wherein said password cookie is encrypted using a shared secret key.

24. (Currently Amended) An apparatus for providing distributed web server authentication, said apparatus comprising:
a plurality of computer systems, wherein each of said plurality of computer systems is coupled to at least one other of said plurality of computer systems, and wherein each of said plurality of computer systems includes:

a processor unit;
a communications unit coupled to said processor unit;
a memory unit coupled to said processor unit; and
a computer program stored in the memory unit, said computer program, which, when executed by the processor unit configures said computer system for:
receiving a request to connect ~~the~~ a valid user to the computer system through the communications unit;
creating a user password cookie using a shared secret key, wherein the shared secret key is shared by each of said plurality of computer systems; and
transmitting the user password cookie to the user.

25. (Currently Amended) A method of providing distributed web server authentication, said method comprising:
receiving, by a web server, a request to connect a user to the web server;
determining if the user is a valid user;
if the user is not valid, then
denying access to the user;
if the user is valid, then,
if a valid user password cookie exists, then,
updating the user password cookie using a shared secret key;
if no valid user password cookie exists, then,
generating the user password cookie using the shared secret key, wherein the web server is part of a common authentication ring having a plurality of web servers, each of the plurality of web servers having the shared secret key;
transmitting the user password cookie to the user; and
connecting the web server to the user.

26. (Original) The method of claim 25, wherein determining if the user is a valid user, comprises:
reading a user credential cookie;
requesting a user identification (ID) and password;
receiving the user ID and password; and
validating the user's identity.

27. (Original) The method of claim 25, wherein determining if the user is a valid user, comprises:
obtaining the user password cookie;
verifying that the user password cookie is valid;
if the user password cookie is valid, then, the user is valid;
if the user password cookie is not valid, then, the user is not valid.

28. (Cancelled)

29. (Currently Amended) The method of claim 26, wherein generating the user password cookie using the shared secret key, comprises:

combining at least the user ID and password with a time stamp; and

encrypting the combined at least user ID, password and time stamp using ~~a~~ the shared secret key.

30. (Original) The method of claim 25, further comprising:

establishing a connection between the web server and a second user using a second user password cookie and the shared secret key.

31. (Original) The computer-readable medium of claim 23, wherein the shared secret key is used by a communication ring comprising a plurality of web servers.

32. (Original) The apparatus of claim 24, wherein said computer program, which, when executed by the processor unit further configures said computer system for:

connecting the user to the computer system.

33. (New) The method of claim 1, further comprising connecting the valid user to the web server.

34. (New) The method of claim 10, further comprising connecting the second valid user to the web server.

35. (New) The method of claim 12, further comprising connecting the valid user to the second web server.